

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Subject Digital Devices: Yeti Desktop Computer,
more fully described in Attachment A.

Case No. MJ24-589

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Subject Digital Devices: Yeti Desktop Computer, more fully described in Attachment A.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. §§ 2252(a)(2), (b)(2)

Offense Description

Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Special Agent Sara K. Blond, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



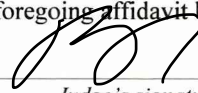
Applicant's signature

Sara K. Blond, Special Agent (FBI)

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 09/19/2024



Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

AFFIDAVIT OF SPECIAL AGENT SARA BLOND

STATE OF WASHINGTON)
)
 COUNTY OF SKAGIT) SS

I, Sara Blond, a Special Agent with the Federal Bureau of Investigation (FBI), in
Seattle, Washington, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I am a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”) and have been so employed since 2009. I am a law enforcement officer of the United States, within the meaning of Title 18, United States Code, who is empowered by law to conduct investigations of, and to make arrests for offenses enumerated in Title 18, United States Code.

2. I am assigned to the Everett and Bellingham Resident Agencies of the FBI's Seattle Field Office, where I specialize in Violent Crimes Against Children and Human Trafficking investigations occurring in Snohomish, Skagit, Whatcom, Island, and San Juan counties, which are situated in the Western District of Washington. I am assigned to the FBI Seattle's Crimes Against Children & Human Trafficking Task Force, which includes investigations of the online sexual exploitation of children involving the transmission, possession and production of child pornography, exploitation of children on the internet, and other federal criminal activity. I am also a member of the Seattle Internet Crimes Against Children Task Force ("Seattle ICAC"). The goal of the Seattle ICAC is to catch distributors of child sexual abuse material (CSAM) on the Internet, whether delivered on-line or solicited on-line and distributed through other channels and to catch sexual predators who solicit victims on the Internet through chat rooms, forums and other methods.

1 3. During my career as an FBI Special Agent, I have served as the case agent
2 in numerous child exploitation investigations. I have participated in all aspects of child
3 exploitation investigations, including conducting surveillance, undercover operations,
4 identifying victims, interviewing suspects, and executing arrest and search warrants. In
5 2015, I underwent specialized training facilitated by the FBI. I successfully completed
6 coursework to become a Digital Evidence Extraction Technician, as authorized by the
7 FBI's Computer Analysis and Response Team. In this capacity, I have specialized
8 training in computer forensics, which involves the search, seizure, and extraction of
9 digital evidence; this requires on-going mandatory training on an annual or semi-annual
10 basis. I have worked as the case agent on numerous investigations involving child
11 pornography, serving as the affiant on search warrants, complaints, and arrest warrants.

12 4. As further detailed below, based on my investigation and the investigation
13 of other law enforcement officers, I believe there is probable cause to conclude that a
14 white Yeti desktop computer, used by KEITH DANIEL FREERKSEN, will contain
15 evidence, fruits, and instrumentalities, of violations of Title 18 United States Code
16 Sections 2252(a)(4)(B),(b)(2) Possession of Child Pornography.

17 5. The information contained in this affidavit consists of my personal
18 knowledge gained through this investigation, information provided by other law
19 enforcement officers involved in this investigation, information provided by witnesses
20 and others with knowledge of the relevant events and circumstances, information gleaned
21 from my review of evidence, and my training and experience. Because this affidavit is
22 offered for the limited purpose of establishing probable cause, I list only those facts that I
23 believe are necessary to support such a finding. I do not purport to list every fact known
24 to me or others as a result of this investigation.

25 **INTRODUCTION AND PURPOSE OF AFFIDAVIT**

26 6. The information contained in this affidavit consists of my personal
27 knowledge gained through this investigation, information provided by other law

1 enforcement officers involved in this investigation, information provided by witnesses
2 and others with knowledge of the relevant events and circumstances, information gleaned
3 from my review of evidence, and my training and experience. Because this affidavit is
4 offered for the limited purpose of establishing probable cause, I list only those facts that I
5 believe are necessary to support such a finding. I do not purport to list every fact known
6 to me or others as a result of this investigation.

7 7. Based on my training and experience and the facts as set forth in this
8 affidavit, there is probable cause to search the following digital device: one white Yeti
9 desktop computer (hereinafter the “SUBJECT DIGITAL DEVICE”) for evidence of
10 violations of Title 18 United States Code Sections 2252(a)(4), (b)(2), Possession of Child
11 Pornography. There is probable cause to believe the SUBJECT DIGITAL DEVICE,
12 which were used by KEITH FREERKSEN, will contain evidence of this crime and
13 contraband or fruits of this crime, as described in Attachment B.

14 **DEFINITIONS**

15 The following definitions apply to this affidavit:

16 8. “Chat,” as used herein, refers to any kind of text communication over the
17 internet that is transmitted in real-time from sender to receiver. Chat messages are
18 generally short in order to enable other participants to respond quickly and in a format
19 that resembles an oral conversation. This feature distinguishes chatting from other text-
20 based online communications such as internet forums and email.

21 9. For the purposes of this affidavit, a “minor” refers to any person less than
22 eighteen years of age and for the purpose of this search warrant, “Child pornography,” as
23 used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit
24 conduct where (a) the production of the visual depiction involved the use of a minor
25 engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer
26 image, or computer-generated image that is, or is indistinguishable from, that of a minor
27 engaged in sexually explicit conduct, or (c) the visual depiction has been created,

1 adapted, or modified to appear that an identifiable minor is engaged in sexually explicit
2 conduct).

3 10. “Sexually explicit conduct” means actual or simulated (a) sexual
4 intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons
5 of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic
6 abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18
7 U.S.C. § 2256(2).

8 11. “Cloud-based storage service,” as used herein, refers to a publicly
9 accessible, online storage provider that collectors of depictions of minors engaged in
10 sexually explicit conduct can use to store and trade depictions of minors engaged in
11 sexually explicit conduct in larger volumes. Users of such a service can share links and
12 associated passwords to their stored files with other traders or collectors of depictions of
13 minors engaged in sexually explicit conduct in order to grant access to their collections.
14 Such services allow individuals to easily access these files through a wide variety of
15 electronic devices such as desktop and laptop computers, mobile phones, and tablets,
16 anywhere and at any time. An individual with the password to a file stored on a cloud-
17 based service does not need to be a user of the service to access the file. Access is free
18 and readily available to anyone who has an internet connection.

19 12. “Computer,” as used herein, refers to “an electronic, magnetic, optical,
20 electrochemical, or other high speed data processing device performing logical or storage
21 functions, and includes any data storage facility or communications facility directly
22 related to or operating in conjunction with such device,” including smartphones and
23 mobile devices.

24 13. “Data,” as used herein refers to the quantities, characters, or symbols on
25 which operations are performed by a computer, being stored and transmitted in the form
26 of electrical signals and recorded on magnetic, optical, or mechanical recording media.

1 14. “Digital Devices” as used herein refers to any physical object that has a
2 computer, microcomputer, or hardware that is capable of receiving, storing, possessing,
3 or potentially sending data.

4 15. “Internet Service Providers” (“ISPs”), as used herein, are commercial
5 organizations, community-owned, non-profit, or otherwise privately-owned companies
6 that are in business to provide individuals and businesses access to the internet. ISPs
7 provide a range of functions for their customers including access to the internet, web
8 hosting, e-mail, remote storage, and co-location of computers and other communications
9 equipment.

10 16. “Mobile applications,” as used herein, are small, specialized programs
11 downloaded onto mobile devices that enable users to perform a variety of functions,
12 including engaging in online chat, reading a book, or playing a game.

13 17. “Records,” “documents,” and “materials,” as used herein, include all
14 information recorded in any form, visual or aural, and by any means, whether in
15 handmade, photographic, mechanical, electrical, electronic, or magnetic form.

16 18. “User Attributes,” as used herein refers to any tangible data, documents,
17 settings, programs, or other information that provides information related to the identity
18 of the specific user of the device, computer, application, program, or record.

19 **INDIVIDUALS WITH A SEXUAL INTEREST IN MINORS**

20 19. Based upon my knowledge, experience, and training in depictions of
21 minors engaged in sexually explicit conduct investigations, and the training and
22 experience of other law enforcement officers with whom I have had discussions, I know
23 that there are certain characteristics common to individuals with a sexual interest in
24 minors who are involved in depictions of minors engaged in sexually explicit conduct as
25 described below.

26 20. Those who possess, receive and attempt to receive depictions of minors
27 engaged in sexually explicit conduct may receive sexual gratification, stimulation, and

1 satisfaction from contact with children; or from fantasies they may have viewing children
2 engaged in sexual activity or in sexually suggestive poses, such as in person, in
3 photographs, or other visual media; or from literature describing such activity. Freerksen
4 has felony convictions in 2017 for multiple counts of possession of child pornography,
5 which resulted in his requirement to register as a sex offender. Based on his prior
6 conviction and coupled with his current charges related to the sexual exploitation of a
7 minor child, there is ample evidence to confirm Freerksen's on-going sexualized interest
8 in minors.

9 21. Those who possess, receive, and attempt to receive depictions of minors
10 engaged in sexually explicit conduct may keep records, to include names, contact
11 information, and/or dates of their interaction, of the children they have attempted to
12 seduce, arouse, or with whom they have engaged in the desired sexual acts.

13 22. Those who possess, receive, and attempt to receive depictions of minors
14 engaged in sexually explicit conduct often maintain their collections that are in a digital
15 or electronic format in a safe, secure, and private environment, such as a computer and
16 surrounding area. These collections are often maintained for several years and are kept
17 close by, usually at the individual's residence, to enable the collector to view the
18 collection, which is valued highly. Again, Freerksen is a convicted sex offender who has
19 maintained a sexualized interest in minors, which he has cultivated by possessing
20 depictions of minors engaged in sexually explicit conduct.

21 23. Those who possess, receive and attempt to receive depictions of minors
22 engaged in sexually explicit conduct also may correspond with and/or meet others to
23 share information and materials; rarely destroy correspondence from other depictions of
24 minors engaged in sexually explicit conduct distributors/collectors; conceal such
25 correspondence as they do their sexually explicit material; and often maintain lists of
26 names, addresses, and telephone numbers of individuals with whom they have been in
27

1 contact and who share the same interests in depictions of minors engaged in sexually
2 explicit conduct.

3 24. Those who possess, receive, and attempt to receive depictions of minors
4 engaged in sexually explicit conduct prefer not to be without their depictions of minors
5 engaged in sexually explicit conduct for any prolonged time period. This behavior has
6 been documented by law enforcement officers involved in the investigation of depictions
7 of minors engaged in sexually explicit conduct throughout the world.

8 **SUMMARY OF PROBABLE CAUSE**

9 25. On or about January 16, 2024, Detective Elizabeth Paul with the Mount
10 Vernon Police Department (MVPD) called me. Det. Paul told me she was assigned a
11 missing persons investigation into Minor Victim, a fourteen-year-old girl, who ran away
12 from home on January 5, 2024. Det. Paul requested I review MVPD's case and help
13 determine an investigative plan. In addition, MVPD requested I evaluate whether there
14 were case-specific facts indicating Minor Victim was a potential crime victim.
15 Beginning that day and continuing over the next two weeks, I read MVPD's reports, and
16 participated in phone calls and meetings with MVPD regarding their investigation. I
17 became familiar with the investigative facts and helped MVPD strategize their next steps.

18 26. Evidence in MVPD's case indicated Minor Victim had an adult male
19 boyfriend known only as "Keith." The timeframe of Minor Victim's relationship with
20 "Keith" was initially unclear. Investigators were not able to determine if "Keith" and
21 Minor Victim were in contact with each other when Minor Victim ran away.

22 27. Information about "Keith" was very limited. MVPD's investigation
23 identified "Keith" as an unconfirmed 30-year-old male that Minor Victim met on
24 Omegle, a website I knew went offline in late 2023 and that the website was suspected by
25 law enforcement agencies of facilitating child abuse. MVPD interviewed several
26 juveniles who were acquainted with Minor Victim. Many of them provided a general
27 physical description of "Keith," and they seemed to be describing the same person.

1 28. MVPD told me that Minor Victim's cell phone was factory-reset by her
2 mother just before Minor Victim ran away. This prevented law enforcement from
3 extracting any forensic data from Minor Victim's phone, meaning any recent
4 communication between Minor Victim and "Keith" was inaccessible to investigators.

5 29. On or about January 31, 2024, Det. Paul called me and said MVPD
6 identified "Keith." MVPD interviewed a friend of Minor Victim, who stated "Keith"
7 sometimes paid for Minor Victim's Uber rides. After identifying a specific Uber ride
8 paid for by "Keith," MVPD served legal process to Uber requesting information on the
9 person who funded that ride. Uber returned the following individual: KEITH
10 FREERKSEN with an accompanying email address and cell phone number.

11 30. MVPD searched law enforcement databases for the phone number
12 associated with Freerksens's Uber account, which resolved to KEITH DANIEL
13 FREERKSEN in South Haven, Michigan. MVPD provided Freerksen's identifying
14 information to me.

15 31. I ran initial records checks on Freerksen. I reviewed Freerksens's criminal
16 history, which showed he was a registered sex offender residing in South Haven,
17 Michigan. Freerksen's criminal history included a felony conviction for possession of
18 child pornography in 2017. The FBI was able to identify Freerksen's car through a
19 records search.

20 32. Then, law enforcement officers searched license plate readers for
21 Freerksen's vehicle during the January 5, 2024, timeframe, which is when Minor Victim
22 went missing. Freerksen's vehicle registered on multiple license plate readers between
23 Michigan and Washington during that period of time. Based on the pattern of the license
24 plate reader hits, it appeared Freerksen traveled westbound through Illinois then Idaho on
25 January 3, 2024, through January 5, 2024. It also appeared that Freerksen traveled
26 eastbound from Idaho to Illinois from January 6, 2024, through January 8, 2024. These
27

1 facts confirmed my belief that Freerksen traveled to Washington from Michigan, picked
2 up Minor Victim, then drove back to his residence in Michigan.

3 33. MVPD installed an emergency ping order on Freerksen's phone. The geo-
4 location data placed the phone in the immediate vicinity of Freerksen's residence in
5 South Haven, Michigan.

6 34. I contacted law enforcement in Michigan with jurisdiction over Freerksen's
7 residence. I spoke to Det. Lt. David Walker with Van Buren County Sheriff's Office
8 and briefed him the investigation into Freerksen and the potential victimization of Minor
9 Victim. I requested his department conduct an imminent welfare check on Freerksen's
10 residence to determine if Minor Victim was inside. Det. Lt. Walker secured a search
11 warrant for Freerksen's residence and assembled a search team.

12 35. When Van Buren County Sheriff's Office executed the search warrant at
13 Freerksen's house on January 31, 2024, they located Minor Victim inside. During a
14 subsequent search of an unfinished outbuilding determined to house Minor Victim and
15 Freerksen, law enforcement located a sex toy and lubricant, among other things.

16 36. During the execution of the same search warrant, law enforcement located
17 numerous digital devices, including two cell phones and one white Yeti desktop
18 computer (the SUBJECT DIGITAL DEVICE). The SUBJECT DIGITAL DEVICE was
19 located inside the outbuilding where Freerksen resided, near a desk under the staircase.

20 37. Other persons who resided on Freerksen's property were interviewed by
21 law enforcement during the search. At least one of Freerksen's family members said
22 Minor Victim and Freerksen were in a romantic relationship. Law enforcement located
23 several articles of clothing that belonged to Minor Victim inside of Freerksen's property.

24 38. Minor Victim was interviewed after her recovery, both during a SANE
25 exam and later by law enforcement. Minor Victim disclosed that Freerksen traveled to
26 Washington, picked her up, and drove her back to Michigan. Minor Victim disclosed she
27 and Freerksen had sex multiple times a day since then. Minor Victim approximated

1 Freerksen sometimes had sex with her as often as ten times a day. Minor Victim defined
2 these sex acts as inclusive of vaginal and oral penetration. Minor Victim disclosed she
3 and Freerksen had sex in a hotel in Idaho shortly after they left Washington.

4 39. Van Buren County Sheriff's Office conducted a forensic examination on
5 the digital devices seized from Freerksen's residence, including the SUBJECT DIGITAL
6 DEVICE. That examination was summarized in a report, which I read. The examination
7 included findings from Freerksen's cell phone and another cell phone Freerksen gave to
8 Minor Victim. Van Buren County Sheriff's Office located nude photos of Minor Victim,
9 as well as videos of Freerksen and Minor Victim having sex. Van Buren County
10 Sheriff's Office also located sexually suggestive text messages between Freerksen and
11 Minor Victim. Some of these conversations occurred in Washington and predated Minor
12 Victim's travel to Michigan.

13 40. Van Buren County Sheriff's Office initiated a search on the SUBJECT
14 DIGITAL DEVICE, but they were unable to extract data due to encryption. Van Buren
15 County Sheriff's Office partnered with other agencies to attempt to bypass the encryption
16 but were ultimately unable to do so.

17 41. On or about September 11, 2024, the SUBJECT DIGITAL DEVICE was
18 transferred from Van Buren County Sheriff's Office's custody into FBI Seattle's custody.
19 The computer is currently secured in FBI Seattle's Evidence Control Center.

20 42. Because cell phones used by Freerksen and Minor Victim already contain
21 CSAM, I believe the SUBJECT DIGITAL DEVICE may also contain CSAM depicting
22 Minor Victim or other children in addition to communications between FREERKSEN
23 and the Minor Victim concerning the travel planned from Michigan to Washington.

24 **TECHNICAL BACKGROUND**

25 43. Courts have recognized that the majority of Americans possess and use
26 cellular telephones, and that most of those keep the phones within their reach at all times.
27

1 Cellular telephones are used for, among other things, voice, text, email, and SMS
2 communications; accessing and posting to social networking websites, surfing the
3 internet, taking, and storing photographs, creating, and storing documents, notes, music,
4 mapping directions to places, etc. Courts have recognized that these devices “smart
5 phones” are essentially small computers with vast storage capacities. Information deleted
6 by the user can be recovered, years after deletion, upon examination of a cell phone’s
7 data.

8 44. Based on my training and experience, I know that the development of
9 computers and portable digital devices in general have revolutionized the way in which
10 those who seek out depictions of minors engaged in sexually explicit conduct are able to
11 obtain this material. Computers serve four basic functions in connection with depictions
12 of minors engaged in sexually explicit conduct: production, communication, distribution,
13 and storage. Additionally, I know that the computer’s capability to store images in digital
14 form makes it an ideal repository for depictions of minors engaged in sexually explicit
15 conduct. The size of the electronic storage media (often referred to as a “hard drive”)
16 used in home computers has grown tremendously within the last several years. Hard
17 drives with the capacity of terabytes are not uncommon. These drives can store
18 thousands of images and/or videos at a high resolution.

19 45. Based on my training and experience and information provided to me by
20 electronic forensic detectives and agents, I know that data can quickly and easily be
21 transferred from one digital device to another digital device via messages, apps, file
22 sharing etc., and via a USB cable or other wired connection. Data can be transferred
23 from computers or other digital devices to internal and/or external hard drives, tablets,
24 mobile phones, and other mobile devices via a USB cable or other wired connection.
25 Data can also be transferred between computers and digital devices by copying data to
26 small, portable data storage devices including USB (often referred to as “thumb”) drives,
27

1 memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical
2 discs (CDs/DVDs).

3 46. Based on my training and experience, collectors and distributors of
4 depictions of minors engaged in sexually explicit conduct also use online, remote,
5 resources to retrieve and store depictions of minors engaged in sexually explicit conduct,
6 including services offered by companies such as Google, Yahoo, Apple, Amazon, and
7 Dropbox, among others. The online services allow a user to set up an account with a
8 remote computing service that provides email services and/or electronic storage of
9 electronic files in any variety of formats. A user can set up, and access, an online storage
10 account from any digital device with access to the Internet. Evidence of such online
11 storage of depictions of minors engaged in sexually explicit conduct is often located on
12 the user's computer or smart phone.

13 47. Based on my training and experience, communications by way of a
14 computer/smart device can be saved or stored on the computer/smart device used for
15 these purposes. Storing this information can be intentional, i.e., by saving an email or
16 saving the location of one's favorite websites in, for example, "bookmarked" files.
17 Digital information can also be retained unintentionally, e.g., traces of the path of an
18 electronic communication may be automatically stored in many places (e.g., temporary
19 files or ISP client software, among others). Examples of this stored data include user-
20 created or saved data, such as contact lists, messages sent and received, images, audio
21 and video files, personal calendars, notes, prescriptions, bank statements, videos,
22 documents, and images; as well as device-generated data, such as user identity
23 information, passwords, usage logs and information pertaining to the physical location of
24 the device over time. Examples of data stored in a smart phone that can reveal a person's
25 location at specific dates and times include metadata and EXIF tags associated with
26 photographs; IP addresses, which are associated with a geographic location; and
27 geographic location associated with the phone sending/receiving signals with cell towers

1 and satellites. As such, a person's use of the smart phone can reveal where a person has
2 been at dates and times relevant to the crime(s) under investigation; a person's activity at
3 relevant dates and times, and/or places a person frequents at which that person is likely to
4 be found for arrest or at which the suspect stored or inadvertently left evidence behind.

5 48. In addition to electronic communications, a user's Internet activities
6 generally leave traces or "footprints" and history files of the browser application used. A
7 forensic examiner often can recover evidence suggesting whether a computer/smart
8 device was using a specific website or application, and when certain files under
9 investigation were uploaded or downloaded. Such information is often maintained
10 indefinitely until overwritten by other data. Additionally, even if such information is
11 deleted from the memory or storage of the device the data may reside on the device for an
12 extended period of time until overwritten by the operating system of the device.

13 49. Based on my training and experience, I have learned that in addition to the
14 traditional collector, law enforcement has encountered offenders who obtain depictions of
15 minors engaged in sexually explicit conduct from the internet, view the contents and
16 subsequently delete the contraband, often after engaging in self-gratification. In light of
17 technological advancements, increasing Internet speeds and worldwide availability of
18 child sexual exploitative material, this phenomenon offers the offender a sense of
19 decreasing risk of being identified and/or apprehended with quantities of contraband.
20 This type of consumer is commonly referred to as a "seek and delete" offender, knowing
21 that the same or different contraband satisfying their interests remain easily discoverable
22 and accessible online for future viewing and self-gratification.

23 50. Based on my training and experience and my consultation with electronic
24 forensic detectives and agents who are familiar with searches of computers and smart
25 devices, I have learned that regardless of whether a person discards or collects depictions
26 of minors engaged in sexually explicit conduct he accesses for purposes of viewing and
27 sexual gratification, evidence of such activity is likely to be located. This evidence may

1 include the files themselves, logs of account access events, contact lists of others engaged
2 in trafficking of depictions of minors engaged in sexually explicit conduct, and other
3 electronic artifacts that may be forensically recoverable.

4 51. Based on my training and experience and my consultation with electronic
5 forensic detectives who are familiar with searches of smart devices, I have learned that
6 offenders will try and obfuscate data containing images and videos of minors engaged in
7 sexual activity. One potential manner of trying to hide the contraband may be by
8 changing file extensions. For example, an image file may often have a file extension of
9 “.jpg” or “.jpeg” signifying that it is an image or photograph. An offender may change
10 the file extension by selecting the “save as” format on a computer or digital device and
11 select “.doc” or “.docx” to make it appear that instead of a contraband image or
12 photograph, it is a word document. The same process may be used to attempt to hide a
13 video file as well. Based on these and other attempts to hide potential contraband, it is
14 necessary for forensic examiners to examine all potential data on the computer.

15 52. Whether some data on the phone is evidence may depend on other
16 information stored on the computer, and the application of an examiner’s knowledge
17 about how a computer operates. Therefore, the context, location, and data surrounding
18 information in the computer’s data may be necessary to understand whether evidence
19 falls within the scope of the warrant.

20 53. I also know based on my training and experience that obtaining subscriber
21 information for a particular device is often useful in determining who possessed the
22 device on a particular date and time. However, a more definitive way to determine the
23 possessor of a device is to examine how the device is used over a period of days or
24 weeks. The content on the device itself, over a period of time, provides vital evidence of
25 the identity of the user of the device; such evidence can be found in communication
26 content, email information, linked social media accounts, photos (selfies), video, and any
27

1 location data on the device. Examination of all this data is necessary to accurately
2 determine who possessed the device at dates and times critical to the investigation.

3 54. I also know based on my training and experience that a search of the digital
4 device itself would irreversibly alter data and/or evidence on the device. The commonly
5 accepted best practice method to search a digital device for evidence involves creating a
6 digital image of the device and then searching that image for the responsive evidence.
7 Creating a forensic image does not alter any evidence on the device; it only copies the
8 data into a searchable format. The image is then searched using search tools to locate and
9 identify that evidence whose seizure is authorized by this warrant. The unaltered device
10 and the image are then preserved in evidence.

11 55. As set forth herein, I seek permission to search for and seize evidence,
12 fruits, and instrumentalities of the above-referenced crimes, and or things or data
13 identifying the individual engaged in the above referenced criminal activity, that might be
14 found in the SUBJECT DIGITAL DEVICE, in whatever form they are found. It has
15 been my experience that individuals involved and interested in depictions of minors
16 engaged in sexually explicit conduct often prefer to store images or videos depicting
17 depictions of minors engaged in sexually explicit conduct in electronic form. The ability
18 to store images of depictions of minors engaged in sexually explicit conduct in electronic
19 form makes digital devices an ideal repository for depictions of minors engaged in
20 sexually explicit conduct.


21 //

22 //

CONCLUSION


56. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

57. Based on the information set forth herein, there is probable cause to search the above-described SUBJECT DIGITAL DEVICE, as further described in Attachment A, for evidence, fruits, and instrumentalities, of violations of Title 18 United States Code Sections 2252(a)(4)(B),(b)(2) Possession of Child Pornography as further described in Attachment B.



SARA K. BLOND
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone on this 19th day of September, 2024.



THE HON. BRIAN A. TSUCHIDA
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant authorizes the seizure and search of the SUBJECT DIGITAL DEVICE, one white Yeti desktop computer and any other electronic storage media found therein the device including internal storage device cards which are currently secured through the FBI Seattle's Evidence Control Center.



ATTACHMENT B

Particular Things to be Seized

The following items, which constitute fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) Possession of Child Pornography, including:

1. All records on the SUBJECT DIGITAL DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2), including:

a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging “app” accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;

b. Evidence of use of the device to communicate with other individuals with a sexualized interest in minors or others about the above-listed crime(s), via incoming or outgoing calls, chat sessions, instant messages, text messages, app communications, social media, SMS communications, and other similar digital communications related to the sexual abuse of a minor or the possession or production of depictions of minors engaged in sexually explicit conduct;

c. Evidence of the identity of the person in possession of the device on or about any times that items of evidentiary value (user attribution evidence), located pursuant to this warrant, were created modified, accessed, or otherwise manipulated. Such evidence may be found in digital communications, photos and video and associated metadata, documents, social media activity, and electronically stored information from the digital device necessary to understand how the digital device was used, the purpose of its use, who used it, and when;

d. Child pornography as defined in 18 U.S.C. § 2256 meaning any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction

1 is a digital image, computer image, or computer-generated image that is, or is
2 indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the
3 visual depiction has been created, adapted, or modified to appear that an identifiable
4 minor is engaged in sexually explicit conduct), in any format or media;

5 e. Evidence of malware that would allow others to control the digital device
6 such as viruses, Trojan horses, and other forms of malicious software, as well as evidence
7 of the presence or absence of security software designed to detect malware; as well as
8 evidence of the lack of such malware;

9 f. Evidence of the attachment to the digital device of other storage devices or
10 similar containers for electronic evidence, and/or evidence that any of the digital devices
11 were attached to any other digital device;

12 g. Evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from a digital device;

14 h. Evidence of times the digital device was used;

15 i. Electronically stored information from the SUBJECT DIGITAL DEVICE
16 necessary to understand how the digital device was used, the purpose of its use, who used
17 it, and when; and

18 j. Information that can be used to calculate the position of the SUBJECT
19 DIGITAL DEVICE, including location data; cell tower usage; GPS satellite data; GPS
20 coordinates for routes and destination queries between the above-listed dates; "app" data
21 or usage information and related location information; and images created, accessed or
22 modified between the above-listed dates, together with their metadata and EXIF tags.
23
24
25
26
27